Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi

Anjar Pradipta
STMIK AMIKOM YOGYAKARTA
e-mail: anjar_pradipta@hotmail.com

Abstract *- One way to secure data or information with the Cryptology. Cryptography is the study of security (secrecy) posts. Technically cryptographic algorithm consists of technical substitution and transposition techniques. Cryptographic techniques can be trusted to handle the security problems of data or information, because in addition to using a computer programming language, cryptography also using mathematical formulas, ranging from the formula simple to complex formulas. From the results of this study concluded that in the absence of a definite formula in Caesar Chiper cryptography method, it can be said that Caesar Chiper difficult to solve.*
Keywords - Cryptography, Caesar, Chiper

Abstrak - Salah satu cara untuk mengamankan data atau informasi dengan Kriptologi. Kriptografi adalah studi keamanan (kerahasiaan) posting. algoritma kriptografi teknis terdiri dari substitusi dan transposisi teknis teknik. teknik kriptografi dapat dipercaya untuk menangani masalah keamanan data atau informasi, karena selain menggunakan bahasa pemrograman komputer, kriptografi juga menggunakan rumus matematika, mulai dari rumus sederhana untuk formula kompleks. Dari hasil penelitian dapat disimpulkan bahwa dengan tidak adanya formula yang pasti dalam metode kriptografi Caesar Cipher, dapat dikatakan bahwa Caesar Cipher sulit untuk memecahkan.
Kata kunci - Kriptografi, Caesar, Chiper

1.a Latar Belakang

Keamanan merupakan aspek penting dari suatu data atau informasi. Dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi. Berbagai cara dilakukan untuk mengamankan data atau pesan tersebut. Salah satu acara untuk mengamankan data atau informasi tersebut dengan Kriptologi. Kriptografi adalah ilmu yang mempelajari tentang pengamanan (kerahasian) tulisan. Karena itu, untuk mengamankan data atau informasi dibutuh suatu cara yang mampu mengatasai masalah keamanan data. Kriptografi sendiri dibagi menjadi 2, yaitu kriptografi klasik dan kriptografi modern. Secara teknik algoritma kriptografi terdiri dari teknik substitusi dan teknik transposisi.

Teknik kriptografi dipercaya dapat menangani masalah keamanan data atau informasi, karena selain menggunakan bahasa pemrograman komputer, kriptografi juga menggunakan rumus-rumus matematika, mulai dari rumus yang sederhana sampai dengan rumus yang kompleks[1]. Dalam kriptografi terdapat dua konsep utama, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana data atau informasi diubah menjadi bentuk yang tidak dikenali sebagai informasi awalnya dengan menggunakan metode tertentu. Sedangkan dekripsi adalah mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Algoritma yang digunakan dalam pengamanan data atau informasi pun beragam jenisnya, seperti Caesar, Abjad Majemuk, DES, IDEA, RSA dan lain sebagainya. Sedangkan pada penelitian ini menggunakan metode Caesar Chiper Abjad Majemuk dalam kriptologi. Caesar Chiper merupakan sistem persandian berbasis substitusi [2]. Enskripsi dan deskripsi pada metode Caesar menggunakan operasi *shift.*
Cara kerja operasi *shift* yaitu dengan mensubstitusikan huruf menjadi huruf pada alfabet yang berada di-*k* sebelah kiri atau sebelah kanan huruf tersebut. Sedangkan chiper alphabet majemuk adalah chiper substitusi ganda yang melibatkan penggunaan kunci berbeda.

1.b Rumusan Masalah

Rumusan rancangan untuk program aplikasi kriptosistem menggunakan metode Caesar Chiper Alphabet Majemuk dengan menggunakan bahasa pemrograman visual FoxPro.

1.c Batasan Masalah

a. Rancangan kriptosistem hanya dapat mengenkripsi dan mendekripsi data yang berupa teks atau tulisan, bukan suara maupun gambar.

b. Ukuran teks yang dapat dienkripsi senilai 254 karakter, teks berupa angka, huruf dan tombol lain yang tersedia pada keyboard, hal ini dikarenakan keterbatasan bahasa pemograman yang digunakan.

1.d Tujuan Penelitian

Untuk mengetahui bagaimana cara merancang Program Kriptografi dengan Metode Caesar Chiper Alphabet Majemuk.

1.e Manfaat Penelitian

Program Kriptografi dengan Metode Caesar Chiper Alphabet Majemuk menghasilkan manfaat dalam peningkatan keamanan data atau informasi.

1.f Metode Penelitian

Metode pebelitian yang digunakan adalah Metode Literatur, dengan mengumpulkan data-data yang diperlukan baik berupa buku, jurnal dan artikel ilmiah yang berhubungan dengan kriptografi.

2.a Dasar Teori

Pengertian kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. *Crypto* berarti secret (rahasia) dan *graphia* berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. dalam perkembangannya, *kriptografi* juga digunakan untuk mengidentifikasi pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital. (*Dony Ariyus, 2005*)

Caesar Chiper

Sebelum ada komputer, kriptografi dilakukan menggunakan pensil dan kertas. Algoritma kriptografi *(chiper)* yang digunakan dinamakan algoritma klasik. Algoritma klasik adalah algoritma berbasis karakter. Dimana enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan kedalam dua macam cipher yaitu :

1. Cipher Substitusi (*Substitution Ciphers*)
2. Cipher Transposisi (*Transposition Ciphers*)

Dalam *Cipher* Substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu unit berarti satu huruf, pasangan huruf, atau kelompok lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah *Caesar cipher* yang digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang ia kirim kepada para gubernurnya.

2.b Kajian Pustaka

Telah banyak penelitian tentang kriptologi klasik. Winantu [3] mengimplementasikan algoritma klasik ke dalam bahasa pemograman PHP. Doni dan Walad [4] membandingkan metode Caesar Chiper dan Vigenere. Hasil dari penelitian tersebut menyebutkan bahwa metode Caesar Chiper semakin kuat karena belum adanya formula yan pasti untuk menghitung panjang kunci yang sebenarnya. Fitriasih, dkk [5] juga meneliti tentang studi model kriptografi klasik. Sasongko [6] membahas pengamanan data informasi dengan menggunakan kriptografi klasik. Hasil dari penelitian tersebut, bahwa dengan menggunakan metode klasik dapat mengamankan data informasi.

3. Analisis dan Perancangan Sistem

Analisis Sistem

Cara kerja sandi Caesar Chiper diilustrasikan dengan membariskan dua set alfabet. Dimana sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (sesuai kunci). Misalkan sandi Caesar Chiper dengan kunci 3, adalah sebagai berikut:

Plainteks : ANJARPRADIPTA
Kunci : p + 3
Chiperteks : DQMDUSUDGLSWD

Sedangkan untuk memecahkan sandi tersebut dengan cara menggunakan kunci sebaliknya, yaitu p – 3. Proses enkripsi (penyandian) dapat dilakukan secara matematis dengan menggunakan operasi modulo. Dimana dengan mengubah huruf-huruf menjadi angka, A = 0, B = 1, ..., Z = 25. Sandi (E_n) dari huruf dengan bergeser *n*. Secara matematis dapat dituliskan dengan rumus.

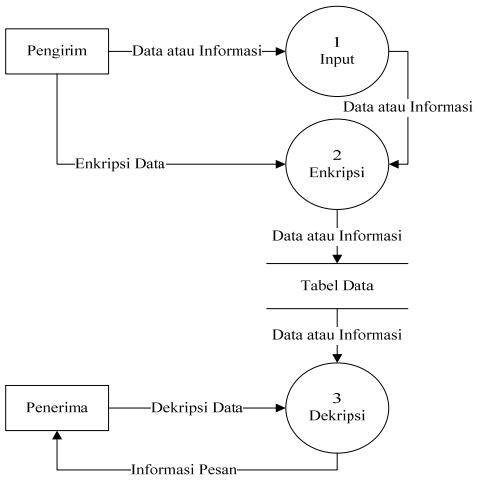
$$E_n(x) = (x+n) \bmod 256$$

Sedangkan untuk proses pemecahan sandi (dekripsi) dapat dituliskan dengan rumus.

$$D_n(x) = (x-n) \bmod 256$$

Perancangan Sistem

Gambar 1 menunjukan gambaran umum dari sistem. Dimana sistem memiliki 3 (tiga) proses, yaitu: input data, enkripsi, dan dekripsi.



Gambar 1. DFD Level 1

Proses pada sistem dimulai dengan menginputkan data yang akan dirahasiakan (enkripsi). Setelah penginputan data atau informasi selesai, kemudian dilakukan proses enkripsi. Data atau informasi hasil dari enkripsi kemudian dikirim pada penerima. Setelah si penerima menerima data atau informasi kemudian dilakukan dekripsi dari data atau informasi yang telah dikrimkan.

4. Implementasi Sistem dan Hasil

Pada penelitian ini aplikasi kriptografi klasik dengan menggunakan metode Caesar Chiper dibuat dengan bahasa pemograman Visual FoxPro.

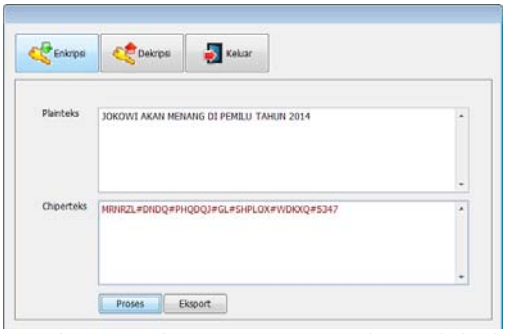
a. Halaman Utama

Pada halaman utama ini berisi menu-menu yang dapat dipilih oleh pengguna. Halaman utama dari aplikasi kriptografi klasik ini seperti Gambar 2 berikut.

Gambar 2. Halaman Utama

b. Halaman Input Data dan Enkripsi

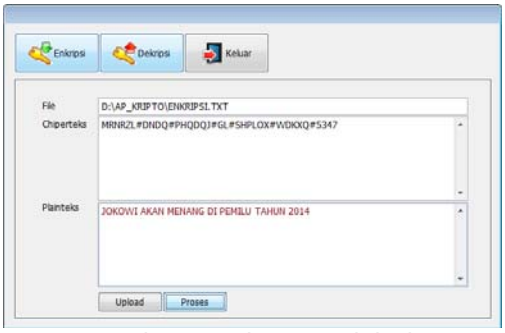
Pada halaman ini pengguna dapat menginputkan data dan melakukan proses enkripsi. Halaman Input Data dan Enkripsi dari aplikasi kriptografi klasik ini seperti Gambar 3 berikut.



Gambar 3. Halaman Input Data dan Enkripsi

c. Halaman Dekripsi

Pada halaman ini pengguna dapat melakukan proses dekripsi. Halaman dekripsi dari aplikasi kriptografi klasik ini seperti Gambar 4 berikut.



Gambar 4. Halaman Dekripsi

4. KESIMPULAN

Dari hasil penelitian dapat disimpulkan, bahwa dengan tidak adanya formula yang pasti dalam metode kriptografi Caesar Chiper, maka dapat dikatakan bahwa Caesar Chiper sulit untuk dipecahkan. Penyandian sangatlah penting dalam mengirim pesan, apalagi pesan tersebut bersifat sangat rahasia.

5. PUSTAKA

[1] Munir, R., 2006, *Kriptografi,* Informatika, Bandung.

[2] Sadikin, R., 2012, *Kriptografi Untuk Keamanan Jaringan,* Andi Offest, Yogyakarta.

[3] Winantu, A., 2010, Implementasi Algoritma Kriptografi Klasik ke Dalam Bahasa

Pemograman PHP, *Fahma Vol 8 No 3, pp 31-44.*

[4] Doni, dan Walad, A., 2012, Caesar Chiper vs Vigenere, *Jurnal LPKIA Vol 1 No 3, pp 12-16.*

[5] Fitriasih, I., Prayitno, TB., Sidopekso, S., 2012, Studi Model Kriptografi Klasik, *spektra Vol 13 Edisi 1, pp 6-11.*

[6] Sasongko, J., 2005, Pengamanan Data Informasi Menggunakan Kriptografi Klasik, *DINAMIK Vol 10 No 3, ISSN 0854-9524, pp 160-167.*